REMARKS

In the final Office Action mailed on January 13, 2005, by the United States Patent and Trademark Office, the Examiner rejected claims 1-15. By way of this Amendment and Reply, Applicants have amended claims 1, 6-8, and 12-15 and have canceled claims 2 and 5 without prejudice. Claims 1, 3, 4, 6-15 remain pending in this patent application. Entry of the foregoing amendments and reconsideration is respectfully requested in light of the following remarks. The foregoing amendments and following remarks are also believed to be fully responsive to the Office Action mailed Janurary 13, 2005, and render all currently pending claims at issue patentably distinct over the cited references.

CLAIM REJECTION UNDER 35 USC §102

At page 2 of this Office Action, claims 8-11 are rejected under 35 U.S.C § 102(e) as being anticipated by U.S. Patent No. 6,584,566 to Hardjono. Applicants submit that amended claim 8 is not anticipated by Hardjono because Hardjono does not disclose all of the elements of Applicants' invention.

Claim 8 is amended to clarify the use of tier-group specific key encryption keys to produce encrypted traffic encryption keys. In particular, claim 8 is amended to recite the steps of:

> "from a list of lower tier key encryption keys, selecting a lower tier key encryption key that does not correspond to a group that includes the compromised node;
>
> encrypting the new traffic encryption key using the lower tier key encryption key, to produce a second encrypted traffic encryption key".

Tier-group specific key encryption keys (KEKs) are used in the claimed invention to encrypt a new traffic encryption key (TEK) when re-keying every node except the compromised node (see Applicants' Specification at page 8, line 26, through page 9, line 23). For example, using a top tier such as tier 2 shown in FIG. 2 and given a compromised node 220, tier-group specific KEK Tier2b is used to encrypt a new TEK that is broadcast to all groups under tier 2b.

Tier-group specific KEK Tier2aTier1a is then used to encrypt a new TEK that is broadcast to all groups under tier 1a.

Although Hardjono teaches using SGK for a multicast to a group of key servers (see Col. 6, lines 25-34), Applicants submit that Hardjono does not teach using tier-group specific key encryption keys (e.g., top tier key encryption keys and lower tier key encryption keys) for encrypting new traffic encryption keys as recited in amended claim 8. In the event of re-keying, Hardjono teaches two methods of notification (see Col. 8, lines 34-56). One method taught by Hardjono uses SGK to multicast to key servers in a server multicast group. The second alternative method taught by Hardjono is using private server specific KSKs. In essence, Hardjono teaches to use a variety of defined group specific keys for distributing a pair of common group keys, namely an initial CGK and a replacement CGK that is swapped out for the initial CGK when re-keying is desired. In contrast with the Applicants' invention, Hardjono takes an entirely different approach to re-keying traffic encryption keys using tier-group specific key encryption keys.

Applicants' respectfully submit that amended claim 8 is patentably distinguished from Hardjono because Hardjono does not teach the use of tier-group (e.g., top tier groups and lower tier groups) specific key encryption keys to encrypt new traffic encryption keys as recited in amended claim 8. Because of the foregoing discussion regarding the patentability of amended claim 8 and because claims 9-11 depend from amended claim 8, Applicants respectfully submit that claims 9-11 are likewise patentably distinguished from Hardjono.

At page 2 of this Office Action, claims 12-15 are rejected under 35 U.S.C § 102(b) as being anticipated by U.S. Patent No. 5,592,552 to Fiat. Applicants submit that Fiat does not disclose all of the elements of Applicants' invention.

Claim 12 is amended to recite as an element "a storage device coupled to the encryption device, the storage device being configured to hold a hierarchy of tier-group specific key encryption keys." Although Fiat discloses a system having n subscriber memories storing a set of keys (see Fiat, claims 17-20), Fiat does not teach or suggest a hierarchy of tier-group specific key encryption keys.

Applicants' respectfully submit that claim 12 is patentably distinguished from Fiat because Fiat does not teach "a storage device being configured to hold a hierarchy of tier-group specific key encryption keys" as recited in amended claim 12. Because of the foregoing discussion regarding the patentability of amended claim 12 and because claims 13-15 depend from amended claim 12 or an intermediate claim depending therefrom, Applicants respectfully submit that claims 13-15 are likewise patentably distinguished from Fiat.

From the foregoing discussion, Applicants respectfully submit that rejection of claim 8-15 under 35 U.S.C. § 102 has been overcome.

CLAIM REJECTION UNDER 35 USC §103

At page 3 of this Office Action, claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,584,566 to Hardjono as applied to claims 8-11 above, and further in view of U.S. Patent No. 6,684,334 to Srivastava and further in view of U.S. Patent No. 6,195,751 to Caronni et al. Claims 2 and 5 are canceled without prejudice. Applicants submit that amended claim 1 is not obviated by Hardjono in view of Srivastava and Caronni et al. because none of the cited references, either alone or in combination, disclose all of the elements of Applicants' invention.

Claim 1 is amended to clarify the use of tier-group specific key encryption keys to produce encrypted traffic encryption keys. In particular, claim 1 is amended to recite the steps of:

> "for each group in a plurality of top tier groups in a top level tier, encrypting a new traffic encryption key using a top tier-group specific key encryption key, wherein the plurality of top tier groups excludes a group that includes the compromised node ...
>
> for each of the groups of nodes in the succession of lower tiers, each of the groups of nodes excluding a lower tier group that includes the compromised node, encrypting the new traffic encryption key using a lower tier-group specific key encryption key [emphasis added]".

As previously set forth hereinabove with regard to the patentability of claims 8-15, tier-group specific KEKs are used in the claimed invention to encrypt new TEK when re-keying

every node except the compromised node. Applicants submit that none of the cited references disclose or suggest using tier-group specific key encryption keys for encrypting new traffic encryption keys.

Srivastava is cited for disclosing a multiple level multicast group. In particular, Srivastava teaches that a group controller generates a new key for a parent of a leaving node as well as all ancestral nodes until the root node is reached. For example, the group controller encrypts a new key of the parent node with the adjacent node/s private key (see Col. 18, lines 49-56). Caronni et al. disclose a system for secure multicast using a first key that is shared with all participant entities and a set of second keys that is shared with a subset of the participant entities. This group key management component stores and maintains the first and second keys in a group key database that is in a non-hierarchical, flat fashion (see Col. 4, lines 41-51). Caronni et al. are cited in this Office Action for disclosing recursive broadcasting.

However, Applicants submit that none of the references, either alone or in combination, discloses or suggests using tier-group specific KEKs to encrypt new TEKs and, at successively lower tiers, broadcast the new TEKs to groups of nodes, excluding the compromised node, until the compromised node is excised.

At page 4 of this Office Action, it is asserted that "Applicant's specification does not define the meaning of the term 'compromised node'". Applicants submit that although the specification lacks text directed to a formal definition of the term "compromised node", Applicants note that the specification refers to "a compromised node" as a node having a valid key that is accessed by an unauthorized user (see Applicants' Specification at page 1, lines 11-23, and at page 4, lines 9-17).

Applicants' respectfully submit that amended claim 1 is patentably distinguished from the cited references, either alone or in combination, because the cited references do not teach nor suggest the steps recited in amended claim 1. Because of the foregoing discussion regarding the patentability of amended claim 1 and because claims 3, 4, 6 and 7 depend from claim 1 or an intermediate claim depending therefrom, Applicants respectfully submit that claims 3, 4, 6, and 7 are likewise patentably distinguished from the cited references.

From the foregoing discussion, Applicants submit that rejection of claims 1-7 under 35 U.S.C. § 103(a) has been overcome.

CONCLUSION

In view of Applicants' amendments and remarks, it is respectfully submitted that the rejections under 35 U.S.C. §102(b) and (e) and §103(a) have been overcome. Accordingly, Applicants respectfully submit that the application, as amended, is now in condition for allowance, and entry of the amendments and such allowance is therefore earnestly requested. Should the Examiner have any questions or wish to further discuss this application, Applicants request that the Examiner contact the Applicants' attorneys at 480-385-5060.

If for some reason Applicants have not requested a sufficient extension and/or have not paid a sufficient fee for this response and/or for any extension necessary to prevent abandonment on this application, please consider this as a request for an extension for the required time period and/or authorization to charge Deposit Account No. 50-2117 for any fee which may be due.

Respectfully submitted,

INGRASSIA FISHER & LORENZ, P.C.

Dated: March 14, 2005

By: _____
Andrew Y. Pang
Reg. No. 40,114
(480) 385-5060